California Man Found Guilty of Conspiracy to Steal Payments from U.S. Department of Defense, Bank Fraud, Lying to Federal Agents, and Other Offenses Related to $23m Phishing Scam

Department of Justice
U.S. Attorney's Office
District of New Jersey
April 29, 2022

CAMDEN, N.J. – A California man was convicted on six counts related to the theft of over $23 million dollars from the U.S. Department of Defense (DoD), money destined for one of its jet fuel suppliers, U.S. Attorney Philip R. Sellinger announced today.

Sercan Oyuntur, 40, of Northridge, California, was convicted on April 28, 2022, of one count of conspiracy to commit wire, mail and bank fraud; two counts of bank fraud; one count of using an unauthorized access device to commit fraud; one count of aggravated identity theft; and one count of making false statements to federal law enforcement officers, following an eight-day trial before U.S. District Judge Joseph H. Rodriguez in Camden federal court.

According to documents filed in this case and the evidence presented at trial:

A corporation that had a contract with the DoD to supply jet fuel to troops operating in southeast Asia employed an individual in New Jersey, who was responsible for communicating with the federal government on behalf of the corporation through a government computer system. Through a complex phishing scheme, Oyuntur and criminal conspirators in Germany, Turkey, and New Jersey targeted the corporation and the individual so that the conspirators could steal money that DoD intended to pay to the corporation for providing jet fuel.

Oyuntur’s conspirators created fake email accounts in other people’s names and designed fake webpages that resembled the General Services Administration’s (GSA) public-facing website. From June to September 2018, the conspirators caused phishing emails to be sent to various DoD vendors, including the individual from New Jersey who represented the corporation, to trick these vendors into visiting the phishing pages. These emails appeared to be legitimate communications from the United States government, but were actually sent by the conspirators, and contained electronic links that automatically took individuals to the phishing pages. There, they saw what appeared to be a GSA website and were prompted to enter their confidential login credentials, which were then used by the conspirators to make changes in the government systems and ultimately divert money to the conspirators.

As part of his participation in the scheme, Oyuntur worked closely with another conspirator, Hurriyet Arslan, who owned a used car dealership, Deal Automotive Sales, in Florence, New Jersey. Arslan opened a separate shell company based in New Jersey for use in the criminal scheme, obtained a cell phone number for the shell company, hired another person to pose as the shell company’s owner, and opened a bank account in the name of the shell company.

California Man Found Guilty of Conspiracy to Steal Payments from U.S. Department of Defense, Bank Fraud, Lying to Federal Agents, and Other Offenses Related to $23m Phishing Scam - GSA Office of Inspector General

On Oct. 10, 2018, based on the fraudulent activities of Oyuntur and his conspirators, DoD transferred $23.5 million that had been earned by the victim corporation into Arslan's Deal Automotive bank account. Arslan went to the bank and was able to access some of this money, but the bank would not release all of the funds to Arslan. That same day, a conspirator in Turkey sent Arslan an email with an altered government contract that falsely indicated Deal Automotive had been awarded a DoD contract valued at approximately $23 million dollars. Oyuntur instructed Arslan to take this fake contract into the bank to explain why he had received the money, so that Arslan could convince the bank to release the remaining funds.

The conspiracy and bank fraud counts of which Oyuntur was convicted each carry a maximum potential penalty of 30 years in prison. The count of using an unauthorized access device to commit fraud carries a maximum potential penalty of 10 years in prison. The false statement count carries a maximum potential penalty of five years in prison. The aggravated identity theft count carries a statutory mandatory consecutive term of two years in prison. The conspiracy and bank fraud counts each carry a maximum fine of equal to the greatest of $1 million or twice the gross profits or loss resulting from the offense, whichever is greatest; the remaining counts carry a $250,000 fine, or twice the gain or loss from the offense, whichever is greatest. Oyuntur will be sentenced on a date to be determined.

Arslan pleaded guilty in January 2020 to conspiracy, bank fraud, and money laundering and is scheduled to be sentenced on June 21, 2022.

U.S. Attorney Sellinger credited criminal investigators of the U.S. Attorney's Office, under the direction of Special Agent in Charge Thomas Mahoney; special agents of the General Services Administration, Office of Inspector General, under the direction of Special Agent in Charge Eric D. Radwick; special agents of the U.S. Department of Defense, Defense Criminal Investigative Service, Northeast Field Office and the Cyber Field Office, under the direction of Special Agent in Charge Patrick Hegarty and Special Agent in Charge Kenneth A. DeChellis; and special agents of the Department of Homeland Security, Homeland Security Investigations, under the direction of Special Agent in Charge Jason J. Molina in Newark, with the investigation leading to today's conviction.

The government is represented by Senior Trial Counsel Jason M. Richardson of the Civil Rights Division in Camden and Assistant U.S. Attorney Sara A. Aliabadi of the Special Prosecutions Division in Camden.

Source: U.S. Attorney's Office press release